**Amendments to the Claims:**

The following will replace all prior versions, and listings, of claims:

**Listing of Claims:**

1. (Previously Amended) An automated encryption system for encrypting an electronic message from a sender to a recipient comprising:

a computer readable medium in communications with a sender's e-mail client;

a set of encrypted private keys associated with senders' ID's and passwords stored in said computer readable medium;

a set of computer readable encryption instructions embodied in said computer readable medium for receiving said electronic message from said e-mail client that is created by the sender and addressed to the recipient having the sender's ID and password, attempting to decrypt the sender's private key according to said sender's ID and password, if the sender's private key is successfully decrypted, attempting to retrieve said recipient's public key from said computer readable medium, the sender's private key is successfully decrypted, but the recipient's public key is not located in said computer readable medium attempting to retrieve the recipient's public key from a PKI server in communications with said computer readable medium if said recipient's public key is located, encrypting said electronic message according to said recipient's public key forwarding said encrypted message to the recipient for subsequent retrieval so that the electronic message is automatically encrypted and delivered to the recipient without the need for the email client

to retrieve the recipient's public key or encrypt the message.

2. (Previously Amended) The system of claim 1 wherein

said set of computer readable encryption instructions include instructions for retrieving said private key associated with the sender from said set of private key data and digitally signing said electronic message from the sender according to said private key associated with the sender so that the recipient can verify the authenticity of said electronic message.

3. (Previously Amended) The system of claim 1 wherein:

said set of computer readable instructions include instructions that if the sender's private key is successfully decrypted but the recipient's public key is not located on said PKI server, attempting to retrieve the recipient's public key from a certificate authority in communications with said computer readable medium.

4-6. (Previously Canceled)

7. (Previously Amended) The system of claim 1 including:

a set of computer readable key maintenance instruction embodied within said computer readable medium for creating a key pair having said at least one public key associated with the sender and a private key associated with said public key and the sender, storing said public key within said set of public key data so that said public key associated with the sender is available for retrieval, receiving a password from the sender, encrypting said private key according to said password, storing said encrypted private key within said private key data so that the sender can retrieve said private key

for decrypting message sent to the sender, and[[,]] deleting said key pair to prevent the sender from decrypting encrypted messages so that an automated key management system is provided for automatically managing key pairs for senders.

8. (Previously Amended) An automated encryption system for decrypting an electronic message from a sender to a recipient comprising:

a computer readable medium in communication with a sender's mail server;

a set of computer readable decryption instructions embodied within said computer readable medium for receiving a recipient's access attempt from a client representing an attempt to retrieve a message sent from the sender to the recipient having recipient's ID and password, attempting to decrypt sender's private key according to recipient's ID and password, if the sender's private key is decrypted, decrypting said message with said sender's private key and forwarding said decrypted message to the recipient.

9. (Previously Amended) The system of claim 8 wherein:

said set of computer readable instructions include instructions for retrieving said public key associated from the sender, attempting to validate said electronic message according to a digital signature associated with said digital signature, and providing the validation results to the recipient so that the recipient can be notified as to the authenticity of the message.

10-12. (Previously Canceled)

13-18. (Canceled)

19. (Previously Canceled)